ISSN: 0974-5823 Vol. 6 No. 2 September, 2021

International Journal of Mechanical Engineering

A BROACH STUDY ON ISSUES IN SOCIAL ENGINEERING ATTACKS ON SOCIAL NETWORKING SITES

Alagappan Annamalai[1], Dr. Ramesh Chandra Poonia[2] ,Dr. Suresh Shanmugasundaram[3]

Research Scholar, Amity University Rajasthan, India
[2]Department of Computer Science, CHRIST (Deemed to be University), India
[3] Professor, Botho University, Botswana

Abstract

The popularity of social networking sites is well known and researched by numerous research scholars. As they are popular means of communication among friends, the family where users generally share pictures, videos etc., the information flow is humongous, which in turn attract cybercriminals. This poses a grave threat on the users personal information which can be disclosed by the users unknowingly. Thus privacy takes centre stage in the social platform. This paper aims to understand the issues and challenges of social networking sites among users. The result of which will be used as a base for providing an independent application or plugin to enhance the security of social networking sites. The survey indicates that a large number of users are not completely aware of the privacy settings in social networking sites.

Keywords:
Social Networking Sites, Personal Information, Security, Techniques, Users.

Introduction

Security is a common term used in many areas, and cybersecurity is a name specific to the cyber computing platform. There is no particular definition for cybersecurity; however, in general terms, it can be defined as security of interconnected systems such as hardware, software and data from threats. The goal of the cybersecurity is to ensure good security posture for infrastructures, connected networks, mobile devices and data stored on these devices from malicious attackers (Rouse, M., Gillis, A., Clark, C, 2020). The evolution of social networking has redefined the way people communicate with one another due to its outreach, ease of operation and simple platforms and have become a part of our everyday life. Social networking sites form the backbone of many industries, and with its technological outreach, it can be coined as either a boon or a bane. With the internet being the backbone of social networking there is enormous data that flows in and out of the social network and is a ticking time bomb in the form of data leak or compromise of social data, which again raises a fundamental question on "how safe is a social networking"? Most social networking platform users are either unaware of their privacy settings or don't care to modify the default settings. Added to this is the limited awareness of what a hacker can do with the data that is public on the user's profile. This leads to query how much aware is the user on information security. (Boyd, M.D., Ellison, N.B, 2007) (Conti, M., Hasani, A., Crispo, B, 2013) (Conti, M., Hasani, A., Crispo, B, 2011). The popularity of social networking sites has also (Dunn, S, 2016) contributed to increasing data breach on the websites and the data being leaked online, too often. This growing inquisitiveness for data on how, what, when, why, where a person's personal data to understand the person more, is also a factor to be blamed for this increasing insecurity. Most social networking sites are built with basic settings with a bright note on data acceptance and publishing mandate. For example, the profiles of most users in Facebook (profile data like name, gender, education etc.) is a public profile which clearly is shared freely to the users, clearly defying the fundamental privacy rights. (Conti, M., Hasani, A., Crispo, B, 2013). Not only this profile data can be used extensively by external or third party vendors or application developers when the user logs in with his social networking ID. In other words, most social networking sites like Facebook cannot really abstain from sharing this information with other networking sites, but also expose the uses private data to other websites. This further boils down to the fact that any compromise on the third party could potentially lead to exploitation on the user's profile. (Conti, M., Hasani, A., Crispo, B, 2013).

Against, this backdrop an attempt is made to review various security elements involved in the social networking sites. Section one introduces the social networking platform, while section two discusses the diverse research carried out by numerous authors on social networking. Section three discusses the methodology adopted for the survey. Section four analyses and discusses the results of the study and lastly section five concludes the paper.

The Evolution of Social Networking Issues

The popularity of social networking sites can be traced back to a decade. Ever since the initial trigger of the first social networking site sixdegress.com, which originated in the 1990s, the trigger contributed to rapid development in the sphere with the likes faceboom, myspace, cyworld, bebo etc., and have all contributed to the current social media mania with millions of subscriptions. Social media can be termed as "media that was designed to share information among users". The information sphere in social media can either be public or private depending on the user's settings and can be bound by the system controls with restrictions, so on and so forth. (Watts, D. J, 2003). The success of social networking has also attracted many researchers on various segments of the social platform and often built on to analyse networking behaviour. (Milgram, S, 1967) (Granovetter, M, 1973) (Milgram, S, 1977) (Granovetter, M, 1983) (Samarti, P., Sweeney, L, 1998) (Newitz, A, 2003) (Arrison, S, 2004) (Leonard, A, 2004) (Sege, I, 2005).

The Privacy Problem

Privacy issues across social information site is a cause of concern for many users. Many researchers study the different aspects of privacy and highlight the dangers involved in the privacy compromise and aim to address them with feasible solutions. Due to the nature of social networking sites, where numerous age groups are hooked to social networking, predominantly the under-age group is at greater risk and could lead to serious concerns in society. Boyd et al. in her paper relating to trust and privacy, in particular, discuss the issues relating to privacy at length. (Boyd, D, 2003). They highlight the importance of privacy and cites the example of the Friendster website and highlights the exploitation of the site by the fakesters site. She also explains the importance of how subtle changes can lead to people changing their behaviour to connect socially and concludes by indicating how firendster has actually uncovered a hornet's nest around public identity, relationship etc. (Boyd, D, 2003) (Gross, R., Acquisti, A, 2005).

Gross and Acquisti identify four characteristics of personal information identification. The first criteria that are discussed are on how many sites use and encourage users to share personal information like private photos, identifiability etc. In the second criteria, they discuss how information like hobbies, interests etc. are shared which may or may not include personal habits like drugs, sexual preferences etc. The third information that they discuss is on providing these access to other websites when the user uses the logins of the primary site like Facebook etc. which act as an extended profile of the user, and lastly, they discuss how these privacy controls can be exploited in detail in the networking section. (Gross, R., Acquisti, A, 2005). The authors also stress the importance of privacy controls and its implications and flag it as a risk and security threat. Gross also articulates that about 82% disclose information freely. Hay et al. extensively discuss the importance of privacy in their paper and highlight the use of external information in identifying anonymous individuals in the friend's group using algorithms. They propose algorithms to determine the unknown entities in the group. (Hay, M., Miklau, G., Jensen, D., Weis, P., Srivastava, S, 2007).

The issue of untrusted social network exchange is another privacy concern. Kacimi et al. study the untrusted exchanges in the networks of Flickr and propose a tailored solution to the problem with a focus on protecting youngsters falling prey to the sites. They present different protocols to identify and preserve information and discuss the various security issues in detail. Their tailored solution for social network applications facilitates the user to ask and/or submit personal opinions while preserving their anonymity. This proposed protocol is based on a friend-to-friend delivery mechanism. (Kacimi, M., Ortolani, S., Crispo, B, 2009). Raising internet privacy concerns, Young and Haase in their study on Facebook indicate that 99.35% of users use real names, 92.2% reveal birthdates, 80.5% their current city and location, and 97% put up their pictures as part of public profile. They also identify that it is the students who are very active on Facebook and use it to the maximum. They study four hypothesis to prove their theory on how social media has both positive and negative impacts on society. (Young, L.A., Wuan-Hasse, A, 2009).

In their solution to the privacy problem, Narayanan and Shmatikov suggest anonymity to ensure privacy protection. The authors propose a framework by analysing privacy and anonymity in social network and introduce a new algorithm targeting anonymised social network group based on network topology. The authors test Twitter and Flickr as the base for doing their online testing of the framework and infer 12% error rate in the form of identifying user overlaps. They also conclude that among the user data collected on both the social networking sites, the percentage of overlapping users are relatively less, indicating a possibility of different names in both the websites. (Narayanan, A., Shmatikov, V, 2009). Considering the various attributes of the social networking, Baden et al. propose a solution in the form of user-defined privacy-based solution which enables the users to exercise more control on who the access needs to be provided. As part of the solution, the group offers the answer in the form of encryption based on the user attributes (ABE or attribute-based encryption) providing users more control in applying restrictions. They term the solution "Persona" (Baden, R., Bender, A., Spring, N., Bhattacharjee, B, Starin, 2009). Mislove et al. base their study on identifying attributes and test them based on similarities to answer the question, if a given quality the attribute can be used to infer the attributes of similar users based on their similarities and likelihood. They examine two sets of data from universities for testing their hypothesis. They conclude that users with similarities are often friends who share similar profiles. They also end with a note that they could infer with an 80% success rate with inputs ranging as little as 20%. They also primarily rise one question on privacy and privacy controls. (Mislove, A., Viswanath, B., Gummadi, K.P., Druschel, P, 2010)

With more and more social networking sites coming into focus, these microblogging sites, the sites also trigger concerns on the sensitivity of the information being decimated. With security concerns on the rise, it is also essential to ensure the proper use of tools to protect the privacy of the user. In one such scenario, Cristofaro et al. base their study on encryption using cryptography tools for the Twitter platform. They test the platform with a tool named “Hummingbird” as a prototype. They conclude with a note of positive testing protecting the privacy of the tweets and followers alike through encrypting the tweets from prying eyes. (Cristofaro, D.E., Soriente, C., Tsudik, G., Williams, A, 2012).In a similar study Yüksel et al. study privacy problem through a different approach and propose a web-based API tool. The tool facilitates downloading data through an automated system for the specific groups based on their social graphs using social graph visualisation algorithm. (Yüksel, A.S., Yüksel, E.M., Zaim, A.H, 2010).

The Data Share Privacy Problem

Many social networking sites rely on advertisements for generating revenue to ensure a sustainable platform. In the process, they willingly share out information with the other websites as part of information provision or information gathering. This leads to serious privacy breaches on the user’s personal information. Bettiol provides some insights into how many social networking sites share personal information data and use it as a medium for advertising and other purposes without getting the users consent, clearly violating privacy laws, unless it is in small print. (Bettiol, M, 2010). The sharing of these personal data also leads to a bigger attack surface in the form of identity theft leading to more serious repercussions. Jin et al. further study this at length in their paper on clone attacks, fake identities with malicious intent and how this plays a vital role affecting the trust relationships between victims and real friends and classify it into two methods of attribute similarity and similarity of friends networks and provides a feasible solution in resolving the issue. (Jin, L., Takabi, H., Joshi, J.B.D, 2011). These threats lead to a bigger problem in the form of a cybersecurity threat.

Not only is the data share invaluable to the third-party applications that base their entire revenue generation in the form of advertisements, the social behaviour of the user on the social platform is also of interest to the social networking service provider themselves. They use the same for providing suggestions based on the user’s online social habits which further translates as privacy compromise. A social site also translates as advertising self on social media. The data captured may also be distributed to other social networking platforms. For instance, the buying of a product can not only cause an immense interest in the product, but the social networking site may also provide suggestions based on the product to entice the user to try out new products effectively acting as a communicating tool. Lucas et al. discuss the use of social networking sites by the service providers at length and provide an encryption solution as a means of protecting social behaviour. Their answer on encryption is also trade off on security mechanism. This active framework further provides legal compliance thus ensuring privacy protection. The solution, however, could be an expensive proposition due to the involvement of cryptography (Lucas, M.M., Borisov, N, 2008).

The Cybersecurity Problem

The digital transformation of communication has effectively brought into the picture a more significant threat in the form of cybersecurity. Social media is no exception, and in fact, it is the prime target for basing social engineering attacks. Numerous authors have discussed these threats on different platforms.

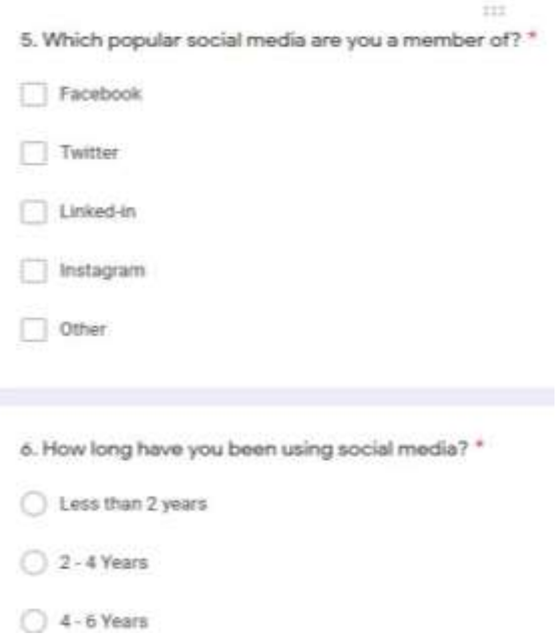
Chewe et al. in their paper, highlight “how personal information is impacted by the internet and social media and discuss the issue of privacy”. They discuss at length the emanating threats affecting users. (Chewae, M., Hayikader, S., Hasan, M.H., Ibrahim J, 2015). Jabee and Alam discuss the issues and challenges of cybersecurity threats in social media platform of Facebook and Twitter at length. They study how users are compromised in sharing their personal information through social engineering attack methods. They base their study on analysing and identifying vulnerabilities in the privacy settings of the user accounts through a survey targeting social media users of the different sphere. The authors formalise the typical social network interface and the information about links that it provides to its users in terms of “lookahead”. In their experiment, they take the case of a specific threat where an attacker sabotages a particular account. In the second stage of the attack, the attacker now tries to gain more information on the network neighbourhoods. On gathering the required information, the attacker then encapsulates the pieces of information together to provide him with a global picture of the user’s profile groups. In this case, it is not only the user’s account that gets compromised by the network of users who are either friends or followers. The authors successfully model and experiment both theoretically and practically and tries to understand the number of user accounts that an attacker would typically subvert. They conclude with a note that the attack is feasible and emphasises the need for greater protection of user accounts and privacy. They further conclude the study inferring that the privacy settings are vital to protecting personal information from cybersecurity attacks. (Jabee, R., Alam, A, 2016).

Gangopadhyay and Dhar, in their article, highlight the importance of security issues and how social networking sites catch the teenagers unaware and unknowingly disclose personal information to unknown people. They study Facebook, myspace, Orkut and twitter as a base and analyse and present their findings (Gangopadhyay, S., Dhar, M. D, 2014). Similarly, Pesce and Casas endorses the research on various types of attacks and discuss at length the various implications of posting private videos, photos in their study on Facebook (Pesce, J.P., Casas, D.L., Rauber, G., Almeida, V, 2012). Gunatilaka emphasises the need for better security in their review on the social networking sites while highlighting the various types of attacks on user profiles like scams, phishing, de-anonymisation attack, neighbourhood attack and so on. . (Gunatilaka, D).

Research Methodology

The aim of this study is to ascertain the awareness among the users of social networking sites, ascertain the vulnerabilities in the privacy settings and to evaluate the associated risks.

The study is based on a well-structured survey questionnaire. Two approaches were adopted for data collection. The survey was circulated to users through google forms and hard copies of the printed form. The questionnaire was divided into two sections, one to understand the demographics and other for awareness. The demographics data included age group, educational qualification, etc., while the security questionnaire was focused towards understanding the awareness of the privacy settings in the social networking sites. The questionnaire comprised of twenty questions out of which five questions were on the demographics while the rest was on social media usage and privacy.



5. Which popular social media are you a member of? *

□ Facebook

□ Twitter

□ Linked-in

□ Instagram

□ Other

6. How long have you been using social media? *

○ Less than 2 years

○ 2 - 4 Years

○ 4 - 6 Years

Figure 1 - Sample Social Media Questionnaire

The survey was circulated using google forms to various email address. Approximately 250 users were sampled for the survey out of which 18 respondents attempted the survey. The survey brought out some interesting results.

Results and Discussion

Demographic Profile

The survey of the 81 respondents who admitted to extensively using social networking sites, 59.3% were males while 40.7% were females. It is interesting to note that 70.4% belonged to the age group between 21-45 indicating the trend that many socially active people belonged to this group, while 21% were below the age of 21 with a meagre 1.2% of the users being above the age of 65 (figure 2). Of the surveyed respondents, 93.8% indicated that they are graduates or completed education up to college or university level, while 4% of the individuals indicated school level (figure 3).

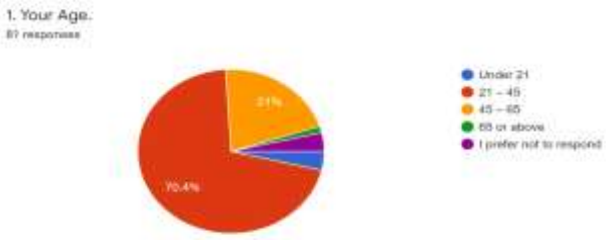


Figure 2 - Age group of surveyed people

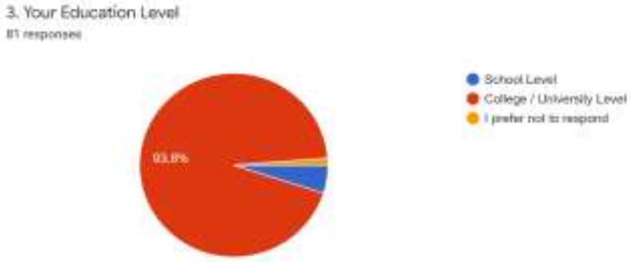


Figure 3 - Education level of surveyed people

Social Media Usage Profile

Of the 81 respondents, 85.2% indicated that they use Facebook extensively. 39.5% indicated twitter, 50.6% linked-in, 21% Instagram, while 13.6% admitted to using other social websites. This indicated that many of the respondents were using multiple social platforms to express their views (figure 4). With respect to the query on the number of years the respondents have been using social media, 43% indicated that they were using social media for over six years, 22% indicated that they have been using it between 4-6 years, while 20% indicated that they have been using it between 2 and 4 years now. It is also important to note that 9% of the users were less than two years indicating that they have recently adopted social media as a platform to express themselves (figure).

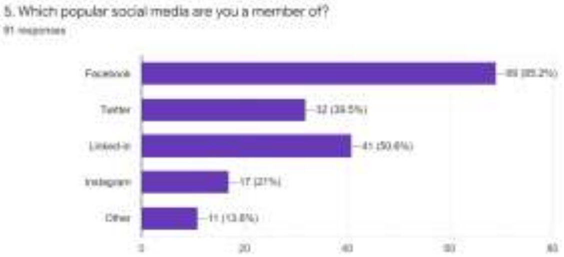


Figure 4 - Social Media profile

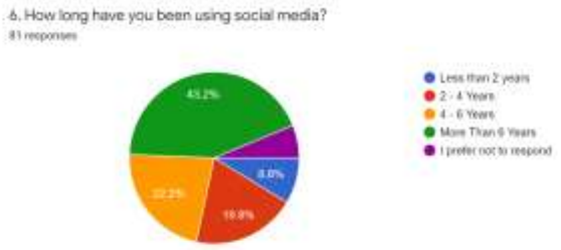


Figure 5 - Social Media usage (years)

The majority of the respondents (77%) indicated that they frequently share their personal photos and videos on the social media platforms while only a meagre 20% indicated that they generally try avoiding posts. The respondents (70%) indicated that they also share pictures of friends and relatives out of which 57% agreed to sharing the location. Though 54% of the respondents indicated that they share personal contact information on the profile, 42% of the respondents answered “NO” to the query on personal information share.

The research also indicated that 73% of the users share personal information on social media, while 23.5% admitted that they generally don’t. On the query of awareness of social security in social media, 83% indicated that they are aware of social risks while 15% of them admitted that they have no idea on the information security in social media. While 88% of the respondents agreed that they don’t share username or passwords with friends or relatives of their profiles, 9% indicated that they do share. This indicates that there is a general awareness among the users on the importance of security, however, there are vulnerabilities from the users sharing information.

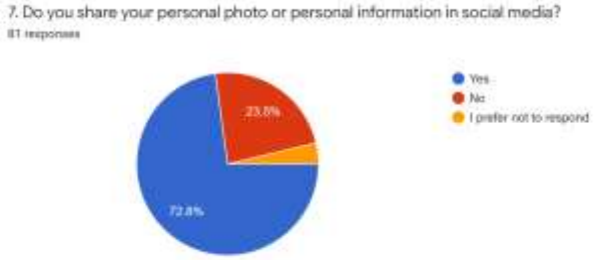


Figure 6 - Information sharing on social media

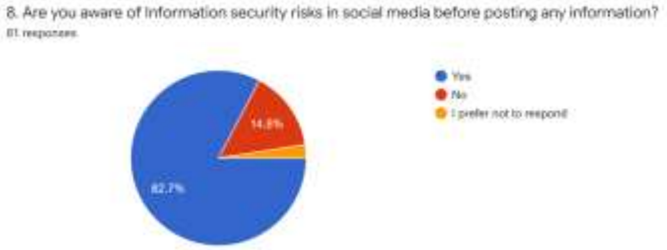


Figure 7 - Awareness of security in social media

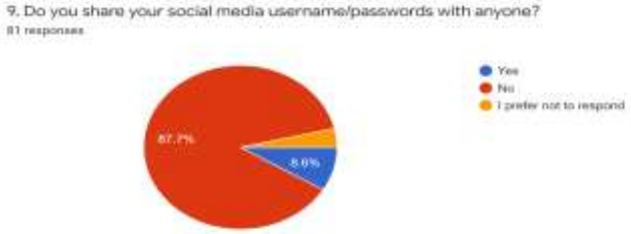


Figure 8 - Credential sharing among users

The research survey also indicated that about 74.1% of the users used security or privacy settings in the social media website Though, majority of the respondents agreed that privacy settings in the social media platforms are a major concern, not many are aware of it as only 23.5% indicated that they hadn’t applied the settings on their profiles.

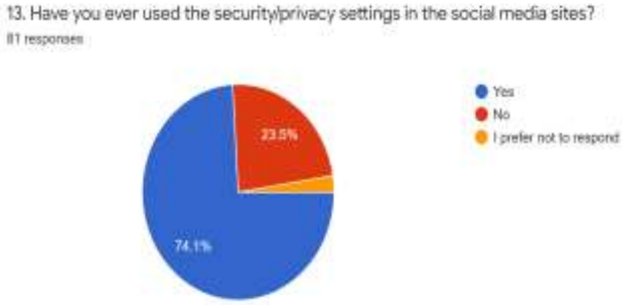


Figure 9 - Application of Security settings in personal profile in social networking sites

Conclusion

This paper discusses privacy settings in virtual private social networks, a concept that can be closely linked to virtual networks. This paper aims to survey the awareness among the social media users to understand the problem of privacy while trying to address this problem through a universal solution in the form a completely independent plugin from the social networking apps while also ensuring anonymity of the users. This study highlights the need for cyber posture improvement in the settings to prevent cyber attacks on private information. As per this survey, the majority of the respondents lie in the age group between 25-40. Though the group, by and large, is aware of their security settings, majority of the users have imminent problems in applying the settings thus providing scope for enhancing the social privacy settings in social networking platforms. This provides a scope for developing an independent application or a plug in to enhance the security in such a way that cannot be modified or interfered by the social networking applications ensuring feasibility.

References

1. Arrison, S. (2004). Friendster in New TIA? *TechCentralStation*.
2. Baden, R., Bender, A., Spring, N., Bhattacharjee, B, Starin. (2009). PERSONA: An Online Social Network With User-Defined Privacy. *SIGCOMM - Data Communication Festival* (pp. 1-7). Barcelona, Spain: ACM Digital Library.
3. Bettiol, M. (2010, May). *Facebook and Others Caught Sending User Data to Advertisers*. Retrieved from bgr.com: https://bgr.com/2010/05/21/facebook-and-others-caught-sending-user-data-to-advertisers/
4. Boyd, D. (2003). Reflections on friendster, trust and intimacy. *Intimate (Ubiquitous) Computing Workshop*. Seattle, Washington: Ubicomp 2003.
5. Boyd, M.D., Ellison, N.B. (2007, October). Social Networking Sites: Definition, History and Scholarship. *Journal of Computer-Mediated Communication, 13*(1), 210-230. doi:10.1111/j.1083-6101.2007.00393.x
6. Chewae, M., Hayikader, S., Hasan, M.H., Ibrahim J. (2015). How Much Privacy We Still Have on Social Network. *International Journal of Scientific and Research Publications, 5*(1), 1.
7. Conti, M., Hasani, A., Crispo, B. (2011). Virtual Private Social Networks. *First ACM Conference on Data and Application Security and Privacy, CODASPY*, (pp. 39-50). San Antonio, TX, USA.
8. Conti, M., Hasani, A., Crispo, B. (2013, September). Virtual Private Social Networks and A Facebook Implementation. *ACM Transactions on the Web, 7*(3), 1-31.
9. Cristofaro, D.E., Soriente, C., Tsudik, G., Williams, A. (2012). Hummingbird: Privacy at the time of Twitter. *IEEE Symposium on Security and Privacy* (pp. 285-299). San Francisco, CA: IEEE Explore. doi:10.1109/SP.2012.26
10. Dunn, S. (2016, December 5). *Social Network Activity*. Retrieved from www.tenable.com: https://www.tenable.com/sc-dashboards/social-network-activity
11. Gangopadhyay, S., Dhar, M. D. (2014). Social Networking sites and privacy issues concerning youths. *Global Media Journal - Indian Edition, 5*(1).
12. Granovetter, M. (1973). The Strength of Weak Ties. *American Journal of Sociology, 78*, 1360-1380.
13. Granovetter, M. (1983). The Strength of Weak Ties: A Network Theory Revisited. *Sociological Theory*, `, 201-233.
14. Gross, R., Acquisti, A. (2005). Information Revelation and Privacy Online Social Network (The Facebook Case). *ACM Workshop in the Electronic Society (WPES)*, 1-8.
15. Gunatilaka, D. (n.d.). *A Survey of Privacy and Security Issues in Social Network.* Retrieved from http://www.cse.wustl.edu/~jain/cse571-11/ftp/social/index.html: http://www.cse.wustl.edu/~jain/cse571-11/ftp/social/index.html
16. Hay, M., Miklau, G., Jensen, D., Weis, P., Srivastava, S. (2007). Anonymising Social Networks. *Computer Science Department and Faculty Publication Series* (pp. 1-18). Scholarworks.umass.edu. Retrieved from https://scholarworks.umass.edu/cs_faculty_pubs/180?utm_source=scholarworks.umass.edu%2Fcs_faculty_pubs%2F180&utm_medium=PDF&utm_campaign=PDFCoverPages
17. Jabee, R., Alam, A. (2016, June). Issues and Challenges of Cyber Security for Social Networking Sites (Facebook). *International Journal of Computer Applications, 144*(3), 36-40.
18. Jin, L., Takabi, H., Joshi, J.B.D. (2011). Towards Active Detection of Identity Clone Attacks on Online Social Networks. *First ACM Conference on Data and Application Security and Privacy* (pp. 27-38). San Antonio, Texas: ACM Digital Library.
19. Kacimi, M., Ortolani, S., Crispo, B. (2009). Anonymous Opinion Exchange over Untrusted Social Networks. *2nd ACM EuroSys Workshop in Social Network System (SNS 09)* (pp. 26-32). ACM Digital Library.
20. Leonard, A. (2004, June). *You are who you know*. Retrieved from Salon.com.
21. Lucas, M.M., Borisov, N. (2008). FlyByNight: Mitigating the Privacy Risks of Social Networking. *2008 ACM Workshop on Privacy in the Electronic Society* (pp. 1-8). Alexandria, VA: ACM Digital Library.
22. Milgram, S. (1967). The Small World Problem. *Psychology Today*, 62-67.
23. Milgram, S. (1977). The Familiar Stranger: An Aspect of Urban Anonymity. (S. S. Milgram, Ed.) *The Individual in a Social World: Essays and Experiments*.
24. Mislove, A., Viswanath, B., Gummadi, K.P., Druschel, P. (2010). You are Who you know inferring user profiles in online social networks. *3rd ACM International Conference on Web Search and Data Mining* (pp. 251-260). New York: ACM Digital Library.
25. Narayanan, A., Shmatikov, V. (2009). De-Anonymising Social Networks. *2009 30th IEEE Symposium on Security and Privacy*, (pp. 173-187). Berkely, C.A.,. doi:10.1109/SP.2009.22
26. Newitz, A. (2003, December). Defenses lacking at social network sites. *Security Focus*.
27. Pesce, J.P., Casas, D.L., Rauber, G., Almeida, V. (2012). Attacks in Social Media Using Photos Tagging Networks: A Case Study with Facebook. *PSOSM: Proceedings of the 1st Workshop on Privacy and Security in Online Social Media*, (pp. 1-8). doi:10.1145/2185354.2185358
28. Rouse, M., Gillis, A., Clark, C. (2020). *What is Cyber Security? Everything you need to know*. (searchsecurity.techtarget.com) Retrieved 09 22, 2020, from searchsecurity.techtarget.com: https://searchsecurity.techtarget.com/definition/cyberse

curity#:~:text=Cybersecurity%20is%20the%20protection%20of,centers%20and%20other%20computerized%20systems.

29. Samarti, P., Sweeney, L. (1998). *Protecting privacy when disclosing information - k-anonymity and its enforcement through generalisation and cell suppression.* SRI International.
30. Sege, I. (2005, April). *Where Everybody Knows your name*. Retrieved from Botston.com.
31. Watts, D. J. (2003). *Six Degrees: The Science of a Connected Age.* W.W. Nortan & Company.
32. Young, L.A., Wuan-Hasse, A. (2009). Information Revelation and Internet Privacy Concerns on Social Network SitesL A Case study of Facebook. *4th International Conference on Communities* (pp. 265-273). Pennsylvania: ACM Digital Library.
33. Yüksel, A.S., Yüksel, E.M., Zaim, A.H. (2010). An Approach for Protecting Privacy on Social Networks. *2010 Fifth International Conference on Systems and Network Communications* (pp. 154-159). Nice, France: IEEE Xplore.